دليلك لتكون آمناً على الإنترنت



محسن حيدر الموسوي

الطبعة الأولى ٢٠٠٩

الإهداء

تعبيراً عن تشجيعي للنهج المتبع في إدارة شركة فوماكو foma-co.com **لتطوير مهارات موظفيها. هذا النهج الذي ينعكس ربحا للموظفين و الشركة معاً، فعندما تتبنى الشركة هذا الأسلوب و تتكلف نقداً ووقتاً، تبني روح انتماء الموظف لها، و تنشر جو من الثقة حول مستقبل الموظف فيها، و تضعه في حالة استقرار نفسي، يدفعه لاعتبار الشركة جزءاً من انجازاته الخاصة، الأمر الذي ينعكس تطويراً مستمراً في العمل و إخراجاً للابداع لدى العاملين، فالابداع هو اهم ما ترتكز عليه الشركات الحديثة في عصرنا هذا لتستمر.**

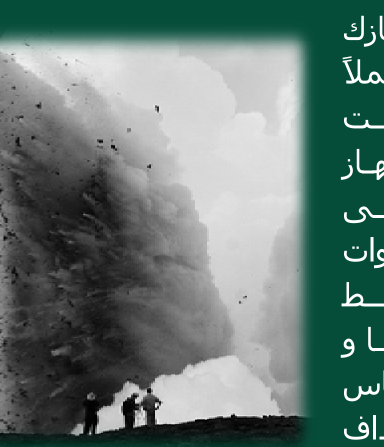
من هذا المنطلق و إيماناً مني أن هذا التطور النوعي لم يكن ليتم لولا مثابرة الأخ حمزة حلباوي و دعم المدير العام الحاج أسامة حلباوي المستمر ، أهدي اليهم هذا العمل البسيط الذي ترجمته بتصرف من دليل شركة Kasper Sky **المختصة بأمن المعلومات** "Your Guide To Stopping Cybercrime". **راجيا أن يستفيد منه كل من يستخدم شبكة الإنترنت لتطوير عمله و بناء مجتمع متطور.**

دليلك لتكون آمنا على الإنترنت

ماذا يقدم لك هذا الدليل

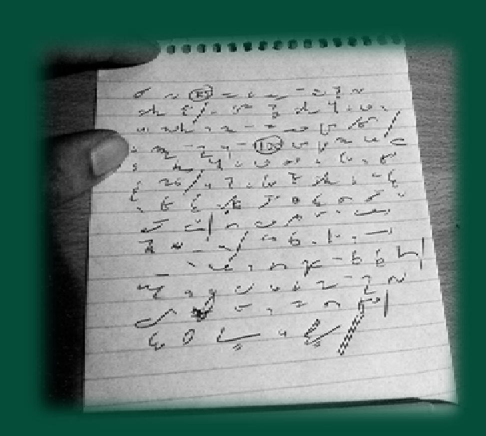
إن هدف هذا الدليل أن يساعدك أن تحمي نفسك من الهجمات على الانترنت، هذه الهجمات تتضمن الفيروسات، الديدان، أحصنة طروادة، هجمات اللصوص، الاحتيال، و المزيد ... أكثر من أي وقت مضى و أكثر تطوراً من ذي قبل هناك أشخاص سيئون يصممون على سرقة هويتك الإلكترونية و جمع بياناتك الشخصية و العمل على غشك. على أية حال، بينما الخطر من الهجمات على الانترنت تواصل نموها، هناك إجراءات وقائية بسيطة تتولد.الإجراءات الوقائية لخصناها في هذا الدليل ، ليكون إبحارك في الانترنت تجربة خالية من القلق و منتجة و ممتعة.

هل الأمر خطير؟



من اللحظة الأولى التي توصل بها جهازك على الانترنت، أنت أصبحت هدفاً محتملاً لجرائم الانترنت، مثلما هو الحال للبيت السائب فهو لقمة سهلة للصوص. فالجهاز الغير محمي يوجه دعوات مفتوحة إلى المبرمجين الخبثاء و جرائمهم. منذ سنوات قليلة ماضية، البرامج الضارة كانت فقط هدفها التخريب، لا شكل اجتماعي لها و كانوا يستغلون ثغرات البرامج و جهل الناس ليقوموا بعمليات تدمير للبيانات لأهداف شخصية و إثبات الذات، في هذه المرحلة كانت معظم البرامج الضارة فيروسات و ديدان. أما اليوم، هناك تهديد أعظم يأتي من شبكة الانترنت، المجرم (الهاكر) تيقظ أن البرامج الضارة من الممكن أن تكون باب لجمع المال، فهو يستعمل هذه البرامج لسرقة البيانات السرية مثل كلمات السر، رقم بطاقات الفيزا، الخ.. أكثر البرامج الضارة اليوم "أحصنة الطروادة"، هناك العديد من الأنواع المختلفة من أحصنة الطروادة، بعضها يسجل كل كبسة تضغطها على لوحة المفاتيح، و أخرى تأخذ لقطة لشاشتك عندما تدخل حسابك المصرفي أونلاين، و بعضها ينشأ اتصال بين جهازك و جهاز لص بعيد، و أخرى تقوم بتنزيل برامج ضارة أخرى. على كل حال، هم جميعا لهم هدف واحد في أرضك المشاع : جمع معلومات عنك يستعملونها لسرقة مالك فيما بعد. هذه الهجمات لم تصبح فقط أكثر تطوراً بل حجمها ينمو، هناك حوالي 17000 تهديد جديد كل يوم، أي ما يقارب ١١ هجوم كل دقيقة.

ماذا تفعل البرامج الضارة Malicious programs



مثل البرامج الأخرى، البرامج الضارة صممت للتصرف على نحو معين و تنفذ بعض الوظائف المعينة، فهم مقيدون بالضبط كأي برنامج آخر. ما يقومون به هو بالضبط ما قام مبرمجهم بكتابته لهم. العديد من الفيروسات القديمة كانت مصممة على الانتشار بسرعة، سبب بعضها آثاراً جانبية غير مقصودة كنتيجة البرمجة السيئة لها، أي عدد قليل نسبياً منها حذف ملفات أو أفسد بيانات، من الممكن أن يكونوا مصدر إزعاج أو سببوا لخسارة بيانات، نعم حاولوا جمع بيانات ليستعملوها في الهجوم التالي. الأمور مختلفة اليوم، البرامج الضارة تتم برمجتها لهدف سرقة معلوماتك، لذلك العديد من برامج "أحصنة طروادة" مدعومة ببرامج تجسس يتم تركيبها على جهازك خلسة منك، بدون معرفتك أو موافقتك، لذلك فهم يراقبون عملك يوماً بعد يوم. هم حريصون للغاية بإخفاء مسار دخولهم لذلك هم يستعملون برامج تسمى root kits . لذلك كل شيء عندك سيعمل بسلاسة و أنت ليس لديك أدنى فكرة عن وجود مشكلة لديك. اليوم برامج التجسس تزرع بجهازك خلسة ، بدون علمك أو موافقتك، و تجمع معلومات شخصية عنك بشكل صامت.

هجوم الهكرز Hackers



التطبيقات التي نستعملها اليوم معقدة جداً، تتكون من آلاف أسطر الكود البرمجي، و الذين يبرمجوها بشر أي غير معصومين، لذلك من الغير مستغرب بأنها تحتوي على أخطاء تعرف بإسم "نقاط الضعف". هذه المنافذ يستغلها لصوص الكومبيوتر "الهكرز" لاقتحام الأنظمة، و تستعمل أيضا من قبل مبرمجي البرامج الضارة لتشغيل برامجهم بشكل أوتوماتيكي على جهازك. أحياناً تستعمل كلمة "هكر" للدلالة على مبرمج ذكي. اليوم يتم استخدامه لكي يقوم باستكشاف نقاط الضعف هذه ليتم الوصول إلى بياناتك. يمكنك أن تعتبره سارق الكتروني يمكنه اقتحام جهاز عادي أو حتى شبكة كومبيوتر كبيرة. و عندما يملك صلاحية الوصول، يقوم على الفور بتركيب برامج ضارة، و يسرق معلومات و يستغل أجهزتك لينشر منها رسائل "سبام"، كما يمكنه استغلال شبكة ليقوم بإغراق موارد شبكة شركة أخرى هذا النوع من الهجوم يسمى هجوم

رفض الخدمة DOS attack، الذي يؤدي بشبكة الشركة المهاجمة لعدم الاستجابة لطلبات جديدة . بالطبع لصوص الكومبيوتر يريدون أقصى استفادة من نقاط الضعف هذه ليخففوا من الجهد و الوقت لذلك يستهدفون أنظمة مستعملة على نطاق واسع، لهذا على سبيل المثال يركزون على نظام التشغيل Microsoft Windows.

كيف احمي نفسي من البرامج الضارة و هجمات الهكرز



هناك عدة خطوات يمكنك أن تأخذها لحماية حاسوبك من تهديدات الانترنت، هذه بعض التعليمات البسيطة ستساعد على تقليل خطر الهجوم:

- أحمي جهازك عبر تركيب برنامج حماية مختص بأمن الانترنت.
- قم بتحديثه و تجديده بانتظام.
- قم بتنصيب رقع الأمن لنظام تشغيلك، إذا كنت تستعمل نظام مايكروسوفت أو لينكس فهذه الآلية بسيطة للغاية، أيضا لا تنسى نفس الأمر مع البرامج الأخرى الموجودة على جهازك.
- إذا استلمت رسالة إلكترونية مرفق معها ملف (مثل ملف وورد،إكسل ...) لا تقم بفتح الملف المرفق إلا إذا كنت تعرف مرسله و تأكد أولا من عنوان بريده الالكتروني، لا تقم أبداً بفتح ملف مرفق من بريد "سبام" هذه القاعدة تنطبق أيضا على الرسائل التي تصلك من برامج المحادثة الفورية مثل Msn Messenger .
- استعمل حساب administrator في نظام التشغيل ويندوز أو حساب root في لينكس فقط في حال كنت تريد تنصيب برنامج جديد أو تطبيق تعديلات على النظام. للاستعمال اليومي قم بإنشاء حساب منفصل بصلاحيات محدودة ، يمكنك ذلك من خلال لوحة التحكم، من خلال هذه الخطوة ستحد من قدرة البرامج الخبيثة على الوصول إلى موارد النظام الثمينة.
- قم بانتظام بنسخة احتياط على قرص مضغوط أو أية وسيلة تخزين أخرى. لذلك فعندما تقوم البرامج الخبيثة بعطب ملفاتك، يمكنك من استعادتها من آخر نسخة احتياط لديك.

باختصار،للحماية من البرامج الضارة و هجمات الهكرز اتبع التالي:

- قم بتركيب برنامج مختص بأمن الانترنت و مضاد للفيروسات.
- قم بتركيب الرقع الأمنية.

- كن على حذر من البريد الإلكتروني الغير مرغوب أو رسائل المحادثة من الغرباء.
- كن حذرا عند تسجيل الدخول على الجهاز بحساب المدير.
- انسخ نسخ احتياط باستمرار.

ما هو الاحتيال Phishing



الاحتيال هو طريقة لسرقة هويتك، لجمع معلومات شخصية عنك بغرض غشك و سرقتك أو القيام عملية سرقة باسمك. "المجرمون الإلكترونيون" يرسلون لك وصلة، عندما تنقرها تأخذك إلى موقع الكتروني شكله مطابق تماماً لموقع بنكك الإلكتروني مثلاً. ثم يحاولون خداعك كي تكتب فيه اسمك و كلمة مرورك و من ثم يستعملون هذه المعلومات لأخذ المال من حسابك المصرفي. نموذجياً "المجرمون الإلكترونيون" يرسلون أعداد كبيرة من الرسائل البريدية الإلكترونية تظهر كأنها تأتي من بنك معين أو مؤسسة مالية، بالطبع، العديد من الناس الذين يستلمون البريد الإلكتروني هذا ليسوا كلهم زبائن المصرف موضع الكلام. لكنه يتوقع أن يتجاوب معه نسبة مئوية صغيرة يستطيع أن يغشها بهدف الحصول على أموالها.تحاول رسائل الصيد الإلكتروني هذه أن تظهر بمظهر البريد الذي يرسله البنك لك عادة و بأسلوبه و شعاره الحقيقي و باستعمال وصلة تتضمن أحيانا اسمك لجعله يبدو كما لو أن البريد الإلكتروني معنون إليك شخصياً. أيضا موضوع الرسالة تكون عادة لسبب مزور، كأن يقول لك بان البنك يقوم بإجراء فحوصات أمنية عشوائية، أو انه يجري تغييرات على بنيته التحتية، في أغلب الأحيان "المجرمون الإلكترونيون" يسحبون كمية معلومات صغيرة نسبياً منك كي لا يثيرون شكك. بالطبع هناك الكثير من الضحايا المحتملين، لذا كمية صغيرة من الكل تعني أرباح كبيرة لهم.

كيف احمي نفسي من عملية احتيال

يجب أن تتبع النصائح السابقة لحماية نفسك من البرامج الضارة و الهكرز. بالإضافة إلى التعليمات التالية التي ستساعدك لتقليل خطر أن تصبح ضحية أحد المحتالين الإلكترونيين .

- لا تكشف معلومات شخصية رداً على رسالة إلكترونية، فمن المستبعد جداً أن يسألك مصرفك عن ذلك برسالة إلكترونية، بل اتصل بهم و دقق بالأمر.
- لا تقوم بنقر الوصلات في رسائل HTML للوصول إلى موقع الويب، هذه الوصلات من الممكن أن تخفي تحتها عنوان مزيف يبدو ظاهره شرعي، بدلا من ذلك قم بكتابة العنوان بنفسك في المستعرض، أو اجعل البرنامج الذي يستلم بريدك الإلكتروني يستعمل النص العادي فقط، فهذه الخدع لن تعمل في النص العادي.



- لا تقم بتعبئة نموذج يرسل لك داخل البريد الإلكتروني، بل في موقع البنك مباشرة، دقق بأن عنوان الموقع هو عنوان البنك بالضبط و ليس شبيها له و ابحث عن رمز القفل في المستعرض للتأكد بأن المعلومات التي ترسلها مشفرة، يمكنك أن تنقر مرتين على هذا الرمز للتأكد من شهادة الضمان المعروضة للموقع الذي تتصفحه، إذا كان لديك أدنى شك استعمل الهاتف لإتمام عملك بدل الانترنت.
- دقق حساباتك المصرفية بانتظام(القيود، بطاقات الائتمان، كشوفات الحساب، الخ ...) للتأكد بأنك أنت من أجرى تلك الصفقات، و أبلغ البنك عن أي شيء مريب يحصل معك.
- كن مرتاباً من أي بريد إلكتروني ليس معنوناً إليك شخصياً، على سبيل المثال يبدأ بـ حضرة الزبون الكريم، أو شيء مماثل.
- كن مرتاباً إذا لم تكن المستلم الوحيد لهذا البريد، فمن الغير المحتمل أن يرسل لك البنك بريد الكتروني متعلق بحسابك الشخصي لأناس آخرون.
- كن مرتاباً من البريد الإلكتروني الذي يحتوي على أخطاء إملائية ونحوي أو استعمال اخرق للغة.

باختصار، للحماية من هجمات الاحتيال عليك بالتالي:

- لا تنقر الوصلات في رسائل بريدك الإلكتروني.
- اكتب بياناتك السرية فقط في موقع البنك مباشرة.

- دقق حسابك المصرفي بانتظام و بلغ عن أي شيء مريب.
- هناك ثلاث إشارات لرسائل الاحتيال:
  1. البريد غير معنون لك شخصياً.
  2. أنت لست المستلم الوحيد.
  3. أخطاء تهجئة و قواعد و غير ذلك.
- اتبع نصائح حماية نفسك من البرامج الضارة و الهكرز السابقة.

هل يصيب الضرر ملفاتي من البرامج الضارة



نعم بعض مجرمي الانترنت يحاولون ابتزاز المال من ضحاياهم الذين يستعملون برامج تطلب فدية. هذه البرامج تقوم بتشفير البيانات و تنشئ ملف "اقرأني Read me" على القرص الصلب يخبرك كيف تستعيد بياناتك لكن فقط إذا دفعت لهم بعض المال مستعملين خدمات الدفع عبر الانترنت مثل e-gold أو WebMoney .

كيف احمي نفسي من برامج الابتزاز

يجب أن تتبع النصائح السابقة لحماية نفسك من البرامج الضارة و الهكرز. بالإضافة إلى التعليمات التالية التي ستساعدك لتقلل احتمال أن تصبح ضحية برامج الابتزاز:

- قم بعمل نسخ احتياط بشكل دوري، البرامج المضادة للفيروسات تستطيع الآن استرداد البيانات المشفرة لكن في المستقبل لا ندري إذا كانت قادرة على ذلك أم لا، على كل حال إذا كانت لديك نسخة احتياط فأنت لن تفقد أية بيانات.
- لا تدفع المال أبدا مقابل استرجاع بياناتك للمجرمين، إذا لم تقم بعمل نسخة احتياط اتصل بفريق الدعم الفني الذي زودك ببرنامج المضاد للفيروسات، فهم خبيرون و قد يساعدونك لاستعادة ملفتك المشفرة.

باختصار، كي لا تكون ضحية ابتزاز:

- انسخ نسخة احتياط دورية.
- لا تدفع المال أبداً للمجرمين.
- اتبع نصائح الحماية من الهكرز و البرامج الضارة.

ما هي برامج الاتصال الغشاشة

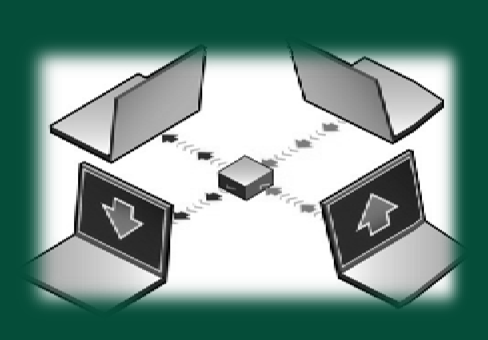
برامج الاتصال الغشاشة تحول مودم جهازك إلى سنترال يتصل بأرقام هاتف معينة للاتصال بالانترنت عوضا عن رقم الهاتف الذي تستعمله للاتصال بمزود خدمة الانترنت ISP الذي تتعامل معه، بحيث يصبح رقم هاتفك من الأرقام التي تتصل بكثافة . هذه البرامج يتم تركيبها بدون معرفة منك أو موافقتك و تعمل سراً. لذا الإشارة الأولى التي تجعلك تشك بهكذا نوع من الاختراق هي فاتورة هاتفك التي ستكون اكبر من المعتاد و فيها أرقام لم تتصل فيها أنت. أيضا هناك رقم هاتف يظهر انك تتصل به باستمرار و أنت لا تعرف عنه شيئاً. يستهدف هكذا نوع من الاختراق الناس الذين يمتلكون اتصال من نوع Dialup أي باستخدام مودم و خط تلفون، إذا كنت تملك اتصال من غير نوع كالاتصال عبر شبكة لاسلكية مثلا فهكذا اختراق لن يكون تهديداً لك، على أية حال عندما تنتقل من خدمة الانترنت عبر الهاتف إلى خدمة Broadband تأكد من فصل سلك الهاتف من المودم و قم بحذف الأيقونة الخاصة بالاتصال عبر الهاتف من نظام تشغيلك، لا تقلق يمكنك إعادة الاتصال من جديد عبر وصل السلك و إنشاء اتصال مرة أخرى. لا تنسى أن برامج الاتصال الغشاشة ستزيد حجم فاتورة هاتفك بشكل ملحوظ.



كيف احمي نفسي من برامج الاتصال الغشاشة

يجب أن تعمل بالنصائح التي مرت مسبقاً حول حماية نفسك من البرامج الضارة و هجمات الهكرز بالإضافة إلى الطلب من شركة الهاتف وضع حظر على أرقام الهاتف التي تبدأ عادة بـ09 أو رقم الهاتف الذي تتصل به هذه البرامج.

كيف احمي شبكة الاتصال اللاسلكية



أجهزة الكومبيوتر الحالية مزودة باتصال لاسلكي تمكنك من الاتصال بشبكة الانترنت من دون كابل. المنفعة الرئيسية منها، هو انه باستطاعتك أن تستعمل حاسوبك في أي مكان من البيت أو المكتب (طالما هو في نطاق التغطية). على أية حال، هناك أخطار محتملة ما لم تضمن أمن شبكتك اللاسلكية .

- إن أي لص كومبيوتر يمكنه اعتراض المعلومات التي ترسلها و تستقبلها.

- إن أي لص كومبيوتر يمكنه من الاتصال بشبكتك اللاسلكية.
- من الممكن أن يسرق شخص أخر اتصالك بالانترنت.

إذا لم تكن الشبكة اللاسلكية آمنة، هذا يعني انك تنشر معلوماتك بالهواء لأي كان! هناك بعض الخطوات البسيطة لتأمين شبكتك اللاسلكية و تخفض نسبة الخطر:

- غير كلمة سر حساب المدير Administrator للـ access point التي تستخدمها، فمن الممكن بكل سهولة أن يحصل المخترق على كلمة السر الافتراضية من المصنع لهذه الآلة و أيضا لا تستعمل كلمات سر من الممكن أن يخمنها بسهولة بل اتبع هذه التعليمات للحصول على كلمة سر قوية:
  - اجعلها من أحرف و أرقام و رموز خاصة.
  - لا تكون اقل من ستة أحرف.
  - غيرها كل فترة.
- قم بتمكين التشفير: تشفير WPA هو الأفضل، إذا كانت مكنتك تدعمه استخدمه ، إذا لا استخدم تشفير WEP .
- قم بتغيير اسم الـ SSID الافتراضية، فمن السهل أن يجد المخترق اسم الافتراضي من المصنّع و يستخدمه لإيجاد شبكتك اللاسلكية. و ابتعد عن الأسماء التي من السهل تخمينها.
- قم بتغيير خاصية البث التي تسمى broadcasting SSID التي تسمح للعالم من حولك أن يعرفوا بوجود شبكتك.
- عندما تشتري جهاز router لاسلكي، اختر واحدا يدعم تقنية NAT ، هذه ستخفي جهازك عن أعين الهكرز، لأنه سيتمكن من رؤية الروتر فقط.

باختصار لحماية شبكة اللاسلكية :

- غير كلمة سر المدير.
- قم بتمكين التشفير.
- أوقف بث الـ SSID و غير الاسم الافتراضي للشبكة.
- اتبع النصائح السابقة للحماية من البرامج الضارة و المخترقين.

ما هو "السبام" spam

السبام هو رسائل من مجهولين، بريد غير مرغوب فيه، النسخة الالكترونية المكافئة لبريد الإعلانات العادي. السبام تصل نسبتها ما بين 70%-80% من حجم البريد الإلكتروني المرسل. السبام تستعمل للإعلان عن السلع و الخدمات، هؤلاء



المعلنون الغير قانونيون يرسلون كم هائل من الرسائل للحصول على المال من أصحاب السلع المعلن عنها ، نموذجياً عدد قليل جداً من مستلمو هذه الرسائل يتجاوبون معها، لكن هذا يكفي للمعلنين أن يحققوا أرباحا منها. هذه الرسائل تسبب الإحباط و ضياع للوقت أثناء تفقدك صندوق بريدك الإلكتروني، و يأخذ مساحة واسعة من صندوق البريد و يستهلك اتصالك بالانترنت، أيضاً هناك نقاط مهمة أخرى:

- السبام من الممكن أن تحمل معها برامج ضارة ملحقة، آو من الممكن تحتوي على رابط لمواقع تحتوي على برامج ضارة (هذه البرامج قد تنزل اتوماتيكيا على جهازك فور زيارتك له في حال كان هناك ثغرة أمنية في جهازك).
- المعلنون هؤلاء قد يستعملون ما يسمى بـ botnets لتوزيع بريدهم الإلكتروني، الـ botnets هي شبكة من الأجهزة المصابة ببرامج ضارة مثل التروجان. الضحية لا يعرف أن جهازه من الممكن أن يتم التحكم به عن بعد، لذلك جهازه سيقوم بإرسال سبام بشكل كبير للآخرين. بالطبع إذا كنت تحمي جهازك ببرنامج امن مضاد للفيروسات سيقلل خطر أن يسيطر على حاسبوك بهذه الطريقة، و لا تنسى أن رسائل السبام من الممكن أن تحتوي على برامج ضارة.

كيف احمي نفسي من "السبام"



يجب أن تتبع النصيحة التي أعطيت من قبل حول حماية نفسك من البرامج الضارة و هجمات لصوص و الكومبيوتر. بالإضافة إلى التعليمات التالية التي ستساعدك على تقليل كمية إغراقك بالبريد الغير مرغوب فيه.

- لا ترد على الرسائل الدعائية أبدا، المعلنون هؤلاء في أغلب الأحيان يسجلون الردود، لذلك سيتأكدون من أن بريدك الإلكتروني صحيح و سيرسلون لك كمية دعاية أكبر في المستقبل.
- أيضاً على تنقر على "عدم الاشتراك في نشرة البريد"، لأنه سيؤكد أن عنوان بريدك نشط، و سيتم استهدافك مجدداً.
- بالنسبة لعناوين بريدك، أبق واحداً للمراسلة الشخصية المهمة، و على الأقل واحد تستعمله للمنتديات العامة، غرف الدردشة، قوائم عناوين و مواقع الويب أو خدمات عامة أخرى، يمكنك استعمال حسابات مجانية متوفرة على الانترنت لهذا الغرض مثل بريد جي ميل آو هوتيمل ... نعم في حال تلقيك كم هائل من

الرسـائل لا يمكـن الـتحكم بها يمكنـك ببسـاطة حـذف هـذا البريـد و إنشاء حساب جديد آخر.

- اجعـل عنـوان بريـدك الإلكترونـي الخـاص صـعب التوقـع. مجموعـات المعلنـين الإلكتـرونيين تـدرج ضـمن مراسـلاتها الأسـماء الواضـحة و كلمـات عنـاوين محتملـة، كـن مبـدعاً و اسـتعمل علـى سـبيل المثـال اسمك و اسم عائلتك.
- تجنب نشر عنوان بريدك الخاص في كل مكان، إذا لم يكن لديك خيار اخفي عنوانك عبر تغيير طريقة كتابة بريدك فبدلا من كتابة my.name@company.com اكتب مثلا: my dot name (at) company dot com، لان المعلنين يستعملون أدوات بحث عن البريد الإلكتروني عبر صفحات المواقع.

باختصار، لتخفيض كمية الرسائل المزعجة:

- لا ترد على الرسائل الدعائية.
- لا تنقر على "عدم الاشتراك".
- استعمل عناوين بريد الكتروني متعددة، واحد للخاص و أخرى للعام.
- لا تنشر بريدك في المواقع.
- اتبع نصائح الحماية من البرامج الضارة و الهكرز.

ما أهمية كلمة السر

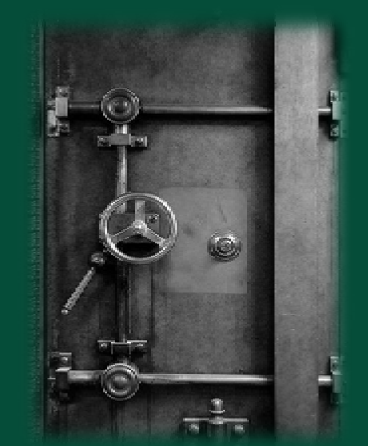


طريـق مهـم تتبعـه عـادة لحمايـة معلوماتـك الخاصـة هـي باسـتعمالك كلمـة للمـرور، هـذا الأمـر أصـبح أكثـر أهميـة بعـد انتشـار اسـتعمال الانترنـت.هنـاك عـدد مسـتخدمين للانترنـت أكثـر مـن ذي قبـل بمختلـف النشـاطات، ضـمن ذلـك الأعمـال المصـرفية، التسـوق عبـر الانترنـت، البحـث عبـر الانترنـت. علـى نحـو متزايـد نحـن نسـتعمل الانترنـت للتواصـل الاجتمـاعي ففـي السـنوات الماضـية نمـت نمـو هائـل مواقـع مثـل MySpace Facebook الـخ... فـنحن نتشـارك فـي تفاصـيل حياتنـا الشخصـية بالإضـافة إلـى الصـور و الموسـيقى و الفيـديو. لسـوء الحـظ ، التفاصـيل الأكثـر شخصـية أصـبحت متـوفرة عنـا للعمـوم، لـذلك مجرمـو سـرقة الهويـة سـوف يحصـلون علـى سـلع و خـدمات بانتحـال اسـمك، علـى سـبيل المثـال يمكنـه فـتح حسـاب مصـرفي، و يحصـل علـى بطاقـة ائتمـان أو يقـدم للحصـول علـى رخصـة قيـادة أو جـواز سـفر. أو ببسـاطة يمكـنهم مـن سـرقة المـال مباشـرة مـن حسـابك المصـرفي. أحـم تلـك المعلومـات الثمينـة بكلمـة مـرور، لكـن كـن حـذراً عنـد اختيـار كلمـة سـر

قوية صعبة التخمين. فكلمة المرور هذه ستحميك من سرقة هويتك الإلكترونية، و تحمي مالك و معلوماتك.

كيف استعمل أفضل كلمات المرور

نعم، من المهم جداً أن تختار كلمة مرور قوية، ففي حال استعملت كلمة سر ضعيفة فأنت تزيد نسبة تحولك إلى ضحية لمجرمي الإنترنت. التزم بالنصائح التي وردت أعلاه، واتبع النصائح التالية ايضا التي ستساعدك على اختيار كلمة سر لحسابك على الانترنت.



- اختر كلمة سر من الممكن أن تتذكرها، لذلك لن تضطر لكتابتها في ملف أو حفظها في جهازك (تذكر أن هذا الملف من الممكن أن يسرق من قبل الهكرز)
- لا تخبر أحدا بكلمة سرك. لأنه اسمها كلمة سر! إذا اتصل بك احد على الهاتف مثلا تحت أي مسمى كان و طلب منك كلمة السر لا تعطه إياها لأنك ببساطة لا تعرف بالضبط من يكون على الطرف الثاني من الخط، أيضا في حال طُلب منك تغيرها إلى كلمة أخرى محددة لا تتجاوب معه.
- إذا أرسل لك متجر الكتروني أو موقع ما على الانترنت بعد تسجيلك فيه كلمة سر عبر البريد الإلكتروني، قم بتسجيل دخولك فورا و غيرها .
- لا تستعمل كلمات سر سهلة التخمين مثل اسم زوجتك، شخصية مهمة، اسم ولدك، اسم حيوانك الأليف، رقم لوحة سيارتك، رقم هاتفك الخ ..
- لا تستعمل كلمة عادية من السهل الحصول عليها عبر قواميس اللغة.
- في حال كانت كلمة مرورك باللاتينية استعمل خليط من الأحرف الكبيرة و الصغيرة، أيضا ضمن كلمة سرك أرقام و رموز الكتابة.
- قدر الإمكان استعمل جملة بدل كلمة واحدة.
- لا تستعمل نفس كلمة السر لأكثر من حساب، فهناك خطر في حال اكتشاف كلمة السر لأول حساب أن يتم اختراق الباقي.
- لا تستعمل التكرار في كلمات السر مثل "كلمة سر1"،"كلمة سر2"،"كلمة سر3" للحسابات المختلفة.
- تأكد من أن برنامج حمايتك يعترض من يحاول سرقة كلمة سرك.

باختصار، عند اختيارك كلمة سر :

- اختر واحدة تتذكرها.

- أبقيها سرية.
- لا تنخدع بكشفها للمحتالين.
- ضمنها أحرف كبيرة و صغيرة و أرقام و رموز.
- لا تستعمل كلمة سر واحدة لأكثر من حساب.
- لا تستعمل التكرار بين كلمات سر مختلفة.
- اتبع نصائح الحماية من البرامج الضارة و الهكرز.

كيف ابقي أولادي بأمان على الانترنت



أول ما يمكن التفكير فيه كأخطار قد تعترض أولادك:



- ما يسمى بالـ drive-by download و هي برامج ضارة تنزل على جهازك فور زيارة موقع سيء.
- خطر الإصابة بالعدوى من برامج المشاركة p2p التي تعطي للآخرين فرصة الدخول إلى جهازك.
- الإعلان الغير مرغوب فيه بما فيها الإعلانات المنبثقة و البرامج المجانية التي تحتوي على إعلانات.
- المحتويات الإباحية و اللاأخلاقية.
- الأطفال من السهل خداعهم لكشف معلومات شخصية عنهم و عنك.
- الأولاد قد يحمّلون على جهازك مواد مسروقة و غير قانونية.
- الأطفال قد يستهدفون من قبل أشقياء الانترنت الغرباء.
- قد يتقرب منهم في غرف الدردشة الشاذين جنسيا.

الأطفال ضعفاء على الانترنت بقدر ما هم ضعفاء في العالم الحقيقي، لذلك يجب توعيتهم.
هناك أشياء يمكن القيام بها لتقليل فرصة تعرضهم لهذه الأخطار:

- تكلم مع أطفالك حول الأخطار المحتملة التي سيواجهونها على الانترنت.
- قدر الإمكان، اجعل الكومبيوتر في غرفة المعيشة مع العائلة و ليس في غرفة منعزلة.
- شجع أطفالك للكلام معك حول أي شيء يواجهونه على الانترنت، فهذا يجعلهم يشعرون بالراحة.
- زودهم بالتعليمات حول ما يمكن أن يسألوا عنه، تذكر بان الإجابات تتغير فيما أطفالك يتقدمون في العمر:
  - هل من الجيد أن أسجل في المواقع الاجتماعية و المواقع المشابهة؟
  - هل من الصحيح أن اشتري من الانترنت؟

- هل من الجيد أن استعمل برامج المحادثة الفورية؟ و مع من أتكلم ؟
- هل باستطاعتي أن أزور مواقع غرف الدردشة؟
- هل من الجيد أن أقوم بتنزيل الموسيقى و الفيديو و البرامج على جهازي؟

- حدد الوصول من جهازك إلى محتويات المواقع، فالعديد من برامج الحماية تتضمن هذه الخاصية، بالإضافة أن برامج التصفح تدعم شيء من هذا القبيل.
- اتبع جميع النصائح السابقة حول الحماية من البرامج الضارة و الهكرز.

باختصار، لحماية أولادك على الانترنت:

- تكلم معهم حول الأخطار المحتملة.
- ابقي الحاسوب في غرفة عائلية.
- شجع الأطفال للكلام حول تجاربهم.
- زودهم بالتعليمات حول النشاط على الانترنت.
- حدد المحتوى الممكن الوصول إليه.
- استخدم النصائح السابقة للحماية من البرامج الضارة و الهكرز.

كيف أتصرف في حال تم اختراق جهازي



ليس من السهل دائما الإخبار إذا كان حاسوبك مخترق، فأكثر من ذي قبل، مبرمجو الفيروسات و الديدان و أحصنة طروادة و برامج التجسس متجهون لإخفاء كودهم و طريقة عمل برامجهم و ماذا تفعل تلك البرامج بأجهزتنا. فمن الضروري إتباع النصائح التي وردت في هذا الدليل، بشكل خاص ركب برنامج أمن و حماية للانترنت و قم بنسخ احتياطي لبياناتك بانتظام. من الصعب جداً تزويدك بقائمة أعراض تبين أن جهازك تم اختراقه، لان نفس العوارض من الممكن أن تكون أيضا سببها أخطاء أجهزة أو مشاكل برامج.

هنا فقط بعض الأمثلة:

- حاسبوك يتصرف بغرابة، و بمعنى آخر بطريقة لم تعتد عليها من قبل.
- ترى رسائل و صور غير متوقعة.
- تسمع أصوات غير اعتيادية و عشوائية.
- برامج تبدأ لوحدها و بشكل اتوماتيكيا.
- برنامج الجدار الناري يخبرك أن هناك برنامج يحاول الاتصال سراً بالانترنت.

- أصدقائك يخبروك بأنهم تلقوا رسائل منك و أنت لم ترسلها لهم.
- جهازك يتجمد كثيراً أو برامجه أصبحت تعمل ببطء.
- تحصل على رسائل خطأ كثيرة من نظام التشغيل.
- عند إقلاع الجهاز لا يتم تحميل نظام التشغيل.
- تلاحظ أن بعض الملفات حذفت أو تغيرت.
- تلاحظ أن القرص الصلب يعمل كثيرا مع انك لا تشغل أية برامج.
- يتصرف مستعرض الانترنت بعصبية و أحيانا لا تستطيع إقفال المستعرض.

لا تضطرب إذا واجهك تلك المشاكل أعلاه، من الممكن انه يوجد عندك مشكلة في العتاد و الأجهزة، أو حتى مشكلة ببرنامج بدلا من الفيروسات، لذلك يجب أن تفعل التالي:

- § افصل حاسوبك عن الانترنت.
- § إذا كان متصلا بشبكة محلية افصله عنها.
- § إذا لم يقلع نظام التشغيل اقلعه في الوضع الآمن safe mode، و قم بنسخة احتياطية.
- § تأكد أن برنامج الأمن عندك لديه آخر تحديث لقاعدة بياناته، لا تقم بتحديثه من الجهاز المصاب بل استعمل جهاز آخر.
- § قم الآن بمسح كامل للجهاز بواسطة برنامج المضاد للفيروسات.
- § إذا وجدت برنامج ضار في جهازك، اتبع التعليمات التي يزودك بها البرنامج المضاد للفيروسات و قم بتطهير ملفات المصابة منه و امحي الديدان و أحصنة طروادة.
- § إذا لم يجد برنامج الحماية لديك برامج ضارة، من المحتمل أن يكون جهازك نظيف لكن فيه مشاكل عتاد أو برامج لذلك قم بإزالة أي عتاد أو برنامج لست بحاجة إليه خاصة تلك المنتهية الصلاحية أو الغير مرخصة.
- § إذا لم تستطع تنظيف جهازك من البرنامج الضار ، ابحث عن أدوات خاصة لنزعه عبر موقع الانترنت الخاص ببرنامج حمايتك.
- § إذا كان الأمر ضروريا اتصل بقسم الدعم الفني لمساعدتك، أيضا من الممكن أن ترسل لهم ملف عينة عن ملف مصاب.

ملاحظة حول سرقة الهوية الإلكترونية



تذكر بأن أمنك و أنت غير متصل مهم أيضا، البيانات على العتاد الصلب مهم أيضا و من الممكن أن يستغل بنفس الطريقة كما هو الحال و أنت أونلاين، فمن الممكن أن تُسرق هويتك الإلكترونية و من الممكن أن يستعملوا بياناتك للدخول إلى حساباتك على الانترنت و يستثمروا باسمك و يخربوا أي

مستند بما فيها المعلومات الشخصية. لذلك لا تعطي صلاحية الوصول إلى جهازك لأشخاص لا تثق بهم، أيضا لا ترمي قرصك الصلب أو قرص مضغوط أو ذاكرة فلاش .. عند الانتهاء من استعماله ، بل قم بتحطيمه إلى قطع بحيث لا يتمكن احد من قراءة هذه المعلومات عنهم.



مواقع مفيدة :

www.kaspersky.com
www.viruslist.com

تم بعون الله تعالى

محسن حيدر نور الدين الموسوي

٢٠٠٩/٥/٢٥

